View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Elsevier - Publisher Connector

JOURNAL OF NUMBER THEORY 3, 33–34 (1971)

Common Divisors of Values of Polynomials

C. R. MACCLUER

Department of Mathematics, Michigan State University, East Lansing, Michigan 48823

Communicated by H. B. Mann

Received February 19, 1970

By checking the factorization in the number field k of the positive rational primes less than the degree of k, it is possible to decide whether or not some integer θ of k has a minimal polynomial $F(X)$ all of whose values $F(x)$ at rational integer x possess a nontrivial common divisor.

Let k be a number field of degree n. Generically let θ be an integer of k of maximal degree n with minimal polynomial $F(X)$ in $\mathbf{Z}[X]$. The positive integer

$$\mathfrak{i}(k) = \underset{\theta \in k}{\text{l.c.m.}}\ \underset{x \in \mathbf{Z}}{\text{g.c.d.}}\ F(x)$$

has been studied in a more general context by Gunji and McQuillan [1]. For instance if $m \neq 1$ is a square free rational integer, then

$$\mathfrak{i}(\mathbf{Q}(\sqrt{m})) = \begin{cases} 2 & \text{if } \ m \equiv 1 \bmod 8 \\ 1 & \text{otherwise} \end{cases}$$

as is not hard to see. An obvious question to ask is: What fields have nontrivial $\mathfrak{i}(k)$? The answer is the following

THEOREM. $\mathfrak{i}(k) > 1$ *when and only when some prime* $p \leqslant n$ *possesses at least* p *distinct factors in* k. *Each and only such primes* p *divide* $\mathfrak{i}(k)$.

Proof. Let θ be any integer of k with field polynomial $F(X)$. Suppose the rational prime p has in k the factorization

$$p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g},$$

where $\mathfrak{p}_i$ is of degree f_i. Then the converse to Kummer's Theorem states that

$$F(X) \equiv F_1(X)^{e_1} \cdots F_g(X)^{e_g} \bmod p,$$

641/3/1-3

where $F_i(X)$ is a monic polynomial of $\mathbf{Z}[X]$ that when taken modulo p becomes the field polynomial for θ modulo $\mathfrak{p}_i$ over $\mathbf{Z}/p\mathbf{Z}$. Note that $F_i(X)$ is of degree f_i and a power modulo p of the irreducible polynomial for θ modulo $\mathfrak{p}_i$.

Suppose p has at least p distinct factors $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_p$, i.e., suppose $p \leqslant g$. Then choose $\theta \equiv i \bmod \mathfrak{p}_i$. To insure that θ is of degree n, let φ be any integer of k of degree n with minimal polynomial $G(X)$ and let $q \neq p$ be any prime not dividing the discriminant of φ. Then $G(X)$ has no repeated roots modulo q. So in addition to choosing

$$\theta \equiv i \bmod \mathfrak{p}_i,$$

require also that

$$\theta \equiv \varphi \bmod q$$

and hence

$$F(X) \equiv G(X) \bmod q.$$

But then $F(X)$ has no repeated roots modulo q, hence no repeated roots. But field polynomials with no repeated roots are irreducible. Thus θ is of degree n and its minimal polynomial $F(X)$ vanishes identically modulo p, i.e., $p \mid \mathfrak{i}(k)$. Conversely, if $p \mid \mathfrak{i}(k)$, merely apply the above converse to Kummer's Theorem.

Reference

1. H. Gunji and D. L. McQuillan, On a class of ideals in an algebraic number field. *J. Number Theory* **2** (1970), 207–222.